

Technical Validation

# Improving Cyber Defenses with SafeBreach

## Continuous Security Validation Powered by the SafeBreach Breach and Attack Simulation Platform

By Justin Boyer, IT Validation Analyst; and Tony Palmer, Principal IT Validation Analyst

September 2022

This ESG Technical Validation was commissioned by SafeBreach and is distributed under license from TechTarget, Inc.

## Introduction

This ESG report details the analysis of SafeBreach’s continuous security validation capabilities, which leverage breach and attack simulation (BAS) to simulate sophisticated, real-world attacks using pre-built and customized scenarios based on real breach methods and TTP (Tactics, Techniques, and Procedures); results of simulations; and in-depth details of how attackers infiltrate systems. ESG also examined how SafeBreach gathers critical data to help organizations prioritize and remediate risk throughout the enterprise.

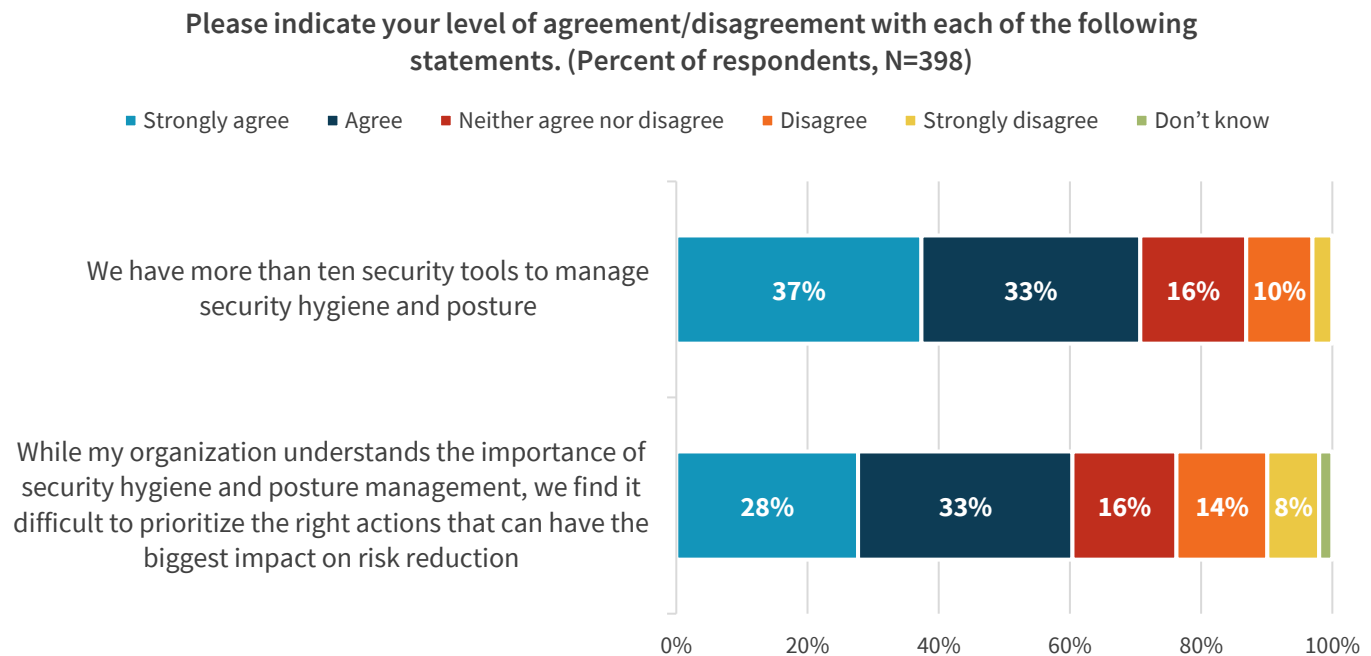
## Background

The number of cyber-threats facing enterprises continues to increase. New vulnerabilities and exploits are discovered every day, adding to the myriad of threats already discovered and catalogued that could still be in use by attackers. These threats force organizations to deploy dozens of security tools requiring trained personnel, leading to greater complexity, higher costs, and overlooked vulnerabilities.

According to ESG research, 70% of organizations use more than ten tools to manage security hygiene and posture (see Figure 1). In addition, 61% find it difficult to prioritize the right actions that can have the biggest impact on risk reduction.<sup>1</sup> Consequently, many enterprises lack a clear picture of their security posture. If they don't know whether their existing defenses are adequate, they certainly wouldn't be able to know the extent to which their organization may be at risk.

Modern enterprises need a safe, efficient, and cost-effective way to determine just how ready they are if an attack occurs, whether their security controls are working as expected, where their greatest weaknesses lie, and what remediations should be addressed first to reduce risk. Modern tools should be easy to use and should offer customization for more advanced users.

**Figure 1. Security Hygiene and Posture Management**



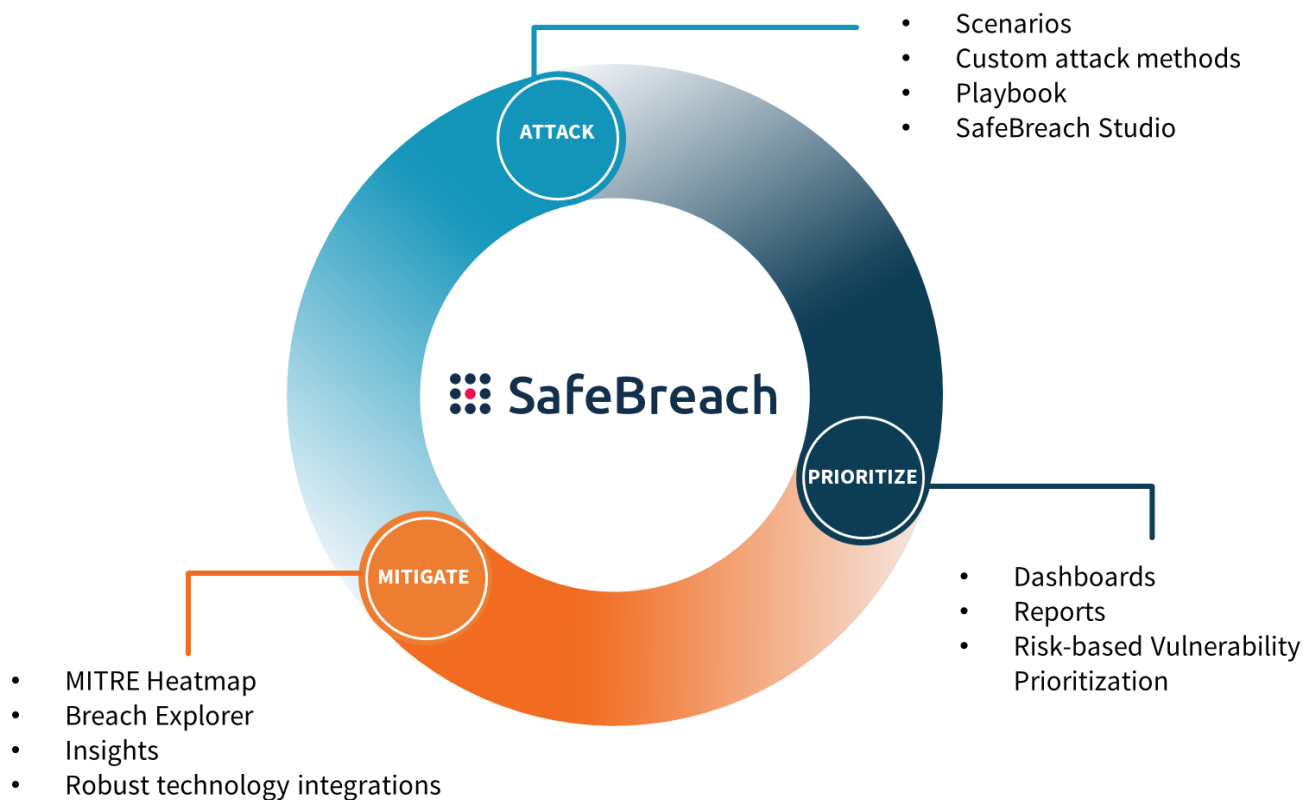
Source: ESG, a division of TechTarget, Inc.

<sup>1</sup> Source: ESG Research Report, [Security Hygiene and Posture Management](#), January 2022.

## SafeBreach’s Breach and Attack Simulation (BAS) Platform

SafeBreach offers continuous security validation powered by BAS. It proactively identifies security risks by simulating real-world attacks on enterprise systems to help organizations validate the efficacy of their security controls and gain visibility into how their security ecosystem responds at each stage of the defense process. With more than 25,000 attack methods, the SafeBreach Hacker’s Playbook includes a 24-hour SLA for the addition of new TTPs and IOCs identified by US-CERT, FBI Flash, and other critical alert platforms. An example of this SLA in action was observed in a recent breach involving a major manufacturer’s network hardware, where SafeBreach researchers quickly developed the actual breach methods used by the attackers and made them immediately available to customers within the platform. The SafeBreach platform offers three main capabilities to help build a complete risk posture for the enterprise (see Figure 2).

**Figure 2. SafeBreach Identifies Security Risk and Informs Decisions**



Source: ESG, a division of TechTarget, Inc.

First, SafeBreach simulates real-world threats using a large playbook of pre-built attacks and scenarios. Customers can create customized attack scenarios using SafeBreach Studio, a no-code red team platform that unifies every aspect of attack planning—from scenario development through execution—in a single, no-code environment. Comprehensive visualization of real-time data outlines how attacks flow throughout a system based on how an attack would try to breach an organization’s defenses. Next, SafeBreach’s Breach Explorer, MITRE ATT&CK board, and Insights module provide in-depth details about how an attacker may infiltrate a system and where the organization successfully stopped attacks. Finally, SafeBreach gathers the results of these simulations into concise, easy-to-understand dashboards and detailed reports to help prioritize the vulnerabilities found, based on their risk to the organization. These in-depth details, along with integrations with downstream tools such as Security Information and Event Management (SIEM); workflow management; and Security Orchestration, Automation, and Response (SOAR) applications help businesses to mitigate risks and protect themselves from real-world attackers. Attacks can be launched on demand or on a schedule, allowing for continuous security control validation.

SafeBreach is simple to deploy. Implementation is based on a representative set of simulator agents which are deployed in the organization and assume the roles of attacker and target. The simulator installation takes just a few minutes and simulators connect to SaaS or on-premises management over standard communication channels. Within a couple of hours, an organization can be up and running and extracting value and insights on security control effectiveness, even with a small number of simulators. With SafeBreach, organizations can see a holistic view of their assets, on-premises and in the cloud, and the risks to those assets.

## ESG Technical Validation

ESG validated SafeBreach’s BAS capabilities via remote demonstration. ESG investigated SafeBreach’s ability to launch attacks through an intuitive user interface and provide comprehensive risk data to help organizations prioritize and mitigate risk.

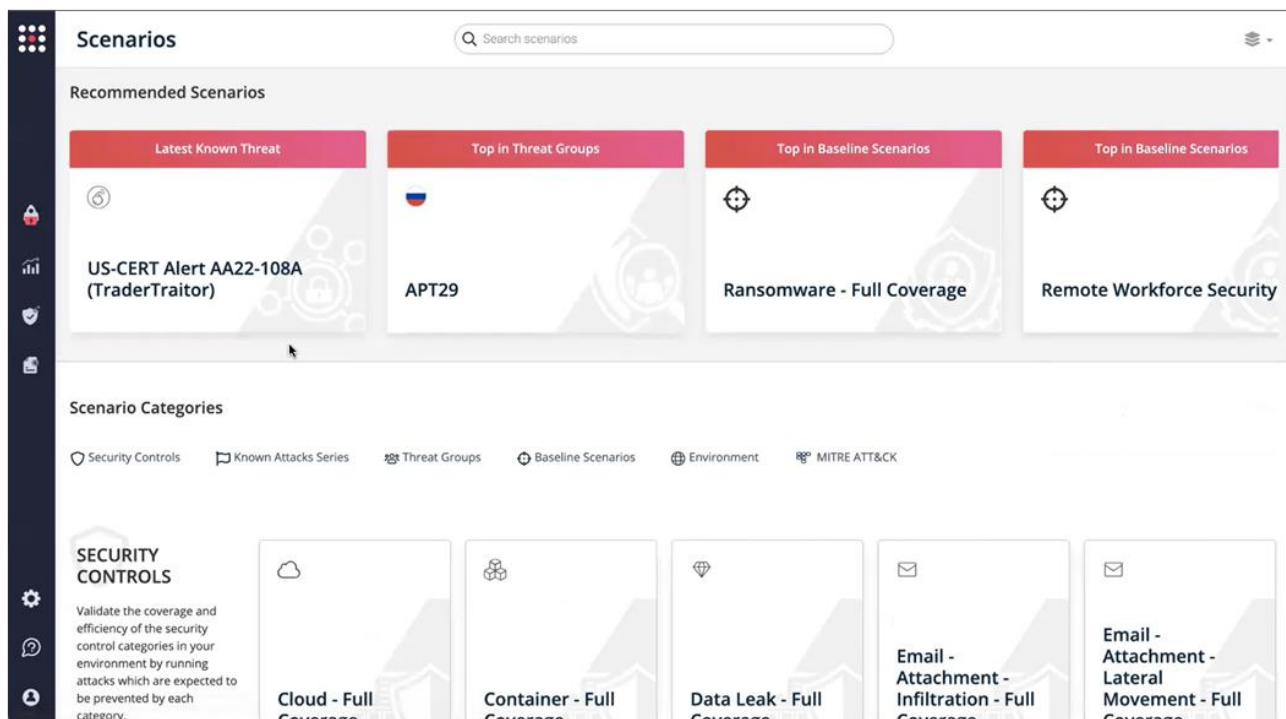
### Launching Sophisticated Attacks

ESG walked through how an organization would launch a simulated attack scenario and discover where it needs to improve its defenses. ESG saw how security administrators can use pre-built attack scenarios or create their own attack methods for testing and how SafeBreach Insights provides a clear picture of the most important weaknesses to address.

### SafeBreach Attack Scenarios

SafeBreach offers over 25,000 attack methods organizations can use to simulate real-world attacks. Security administrators start with SafeBreach’s attack scenarios (see Figure 3). These scenarios use attack simulators built to run with no impact on existing systems. The simulators attack each other across the organization’s environment with real payloads and record what would happen in the event of a real attack. SafeBreach then cleans up after the simulation, leaving no artifacts behind.

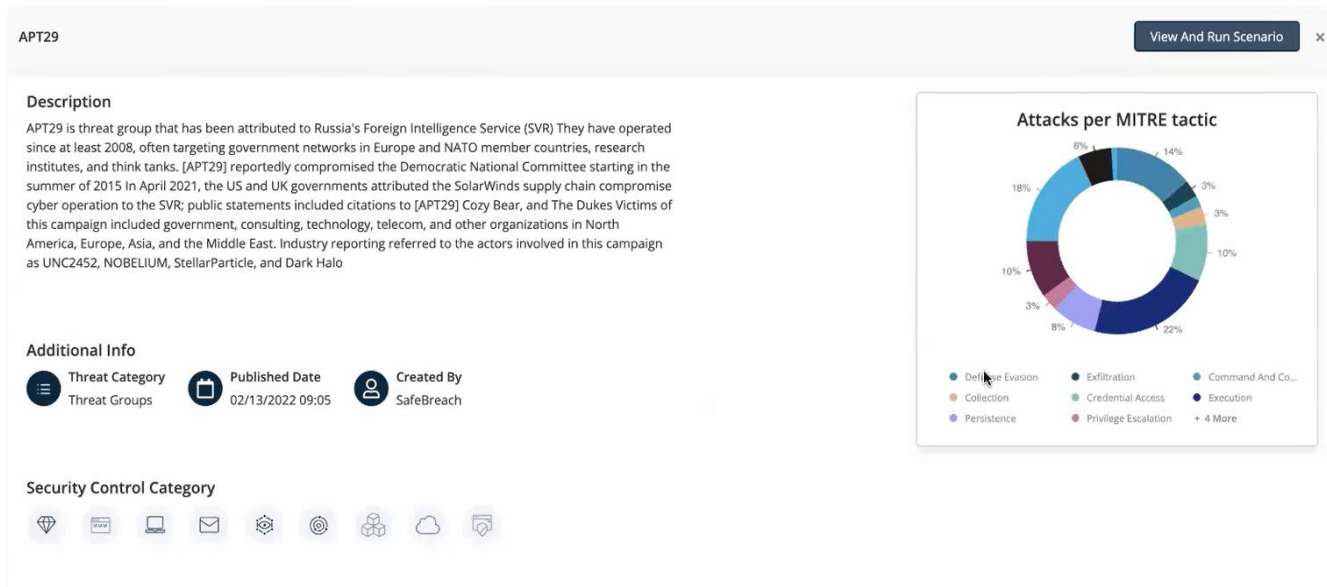
Figure 3. SafeBreach Scenarios



Source: ESG, a division of TechTarget, Inc.

When a security administrator selects a scenario, they will see a comprehensive description of that scenario at a high level and an overview of the attack methods used for that scenario (see Figure 4).

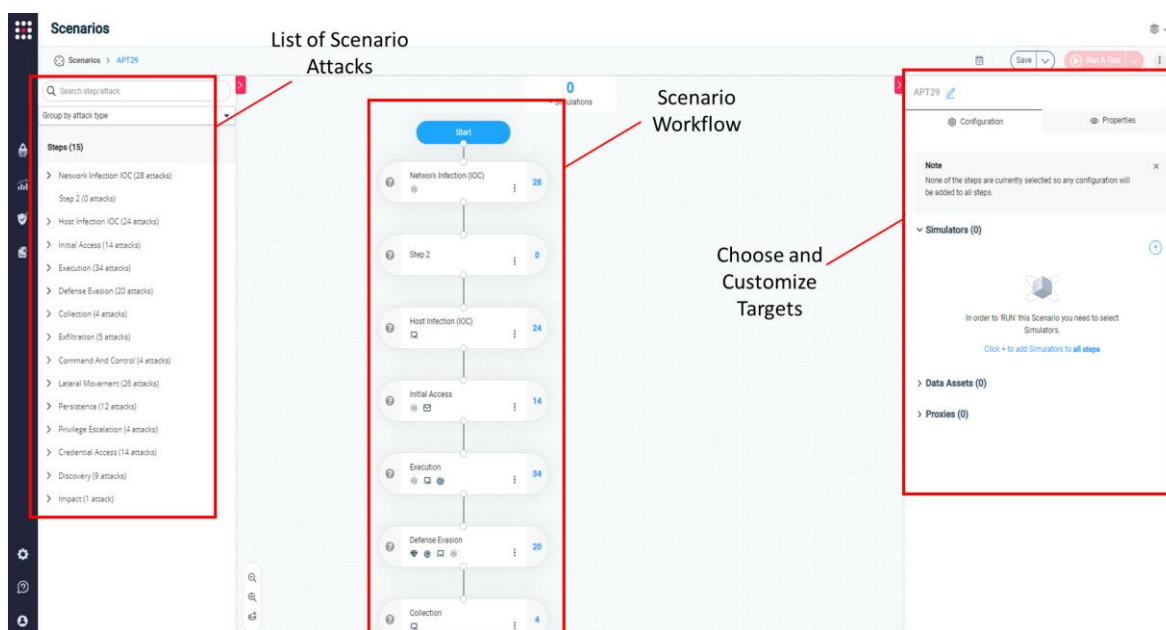
**Figure 4. Attack Scenario Breakdown**



Source: ESG, a division of TechTarget, Inc.

If the administrator chooses to run the selected scenario, they can configure and customize it and select their target simulators using a simple interface (see Figure 5). These simulators help to define a specific scope of attack, such as all corporate Windows servers or a specific cloud environment. It's possible to choose all simulators to run the selected scenario across all assets.

**Figure 5. Attack Scenario View**



Source: ESG, a division of TechTarget, Inc.

## Why This Matters

“Are we safe?” is a simple question, yet it is difficult to answer for most modern organizations. Cybersecurity is a moving target. To be truly safe, organizations need visibility into not just their risk level, but their specific vulnerabilities with the context to prioritize them. Without this knowledge, it’s challenging to know if an organization is safe from the extensive and expanding methods used by attackers to gain access to systems. It’s also difficult to know if the organization’s existing controls offer the needed coverage and effectiveness.

ESG validated that SafeBreach provides an advanced suite of attack methods based on real-world scenarios, including advanced persistent threats and ransomware, providing critical insight to organizations on the coverage and effectiveness of their existing controls.

SafeBreach allows organizations to simulate advanced threats quickly and easily, with the ability to run attack simulations on a regular schedule. This automation helps to reduce dependency on expensive consultants or the need to spin up internal red teams to perform similar testing, and it accomplishes it much faster. The 24-hour SLA provides assurance that the environment can be tested almost immediately after a new exploit comes to light, giving companies the chance to protect themselves.

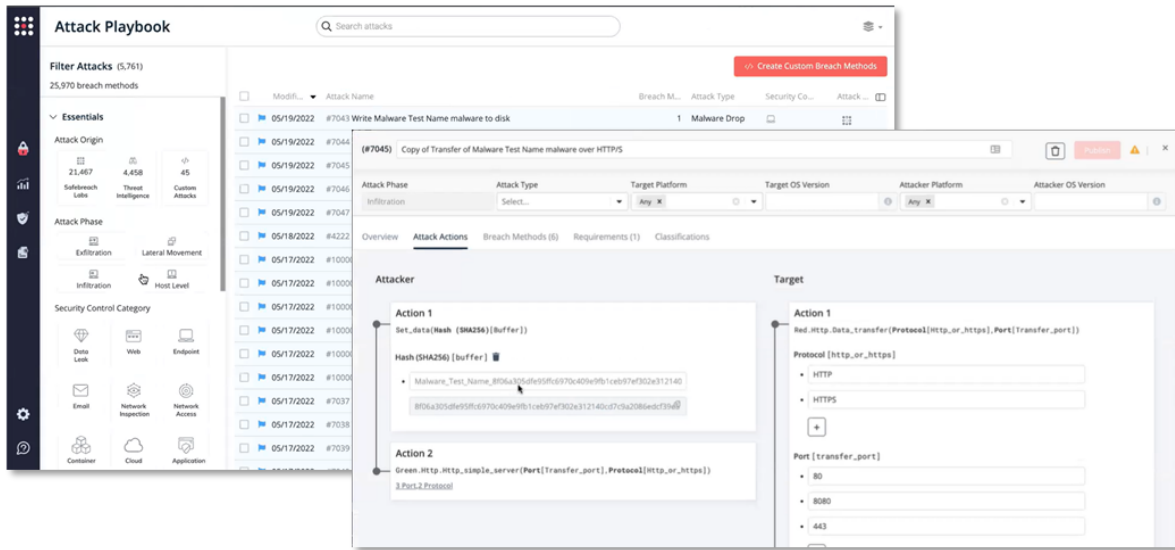
## Extensibility for Advanced Users

Some organizations already have advanced threat intelligence capabilities and red team resources available to actively test their environment. ESG explored the ways in which these more advanced users can use SafeBreach to identify security gaps using their own methods.

### Custom Attack Methods

SafeBreach’s pre-built scenarios allow for point-and-click attack simulation. The Hacker’s Playbook and SafeBreach Studio serve to provide advanced users with maximum extensibility. The Attack Playbook displays individual attacks which can be simulated individually or grouped together as the administrator desires. Figure 6 shows the configuration screen for a specific attack in the playbook. These attacks can be copied, duplicated, and customized to change protocols, ports, or payloads used.

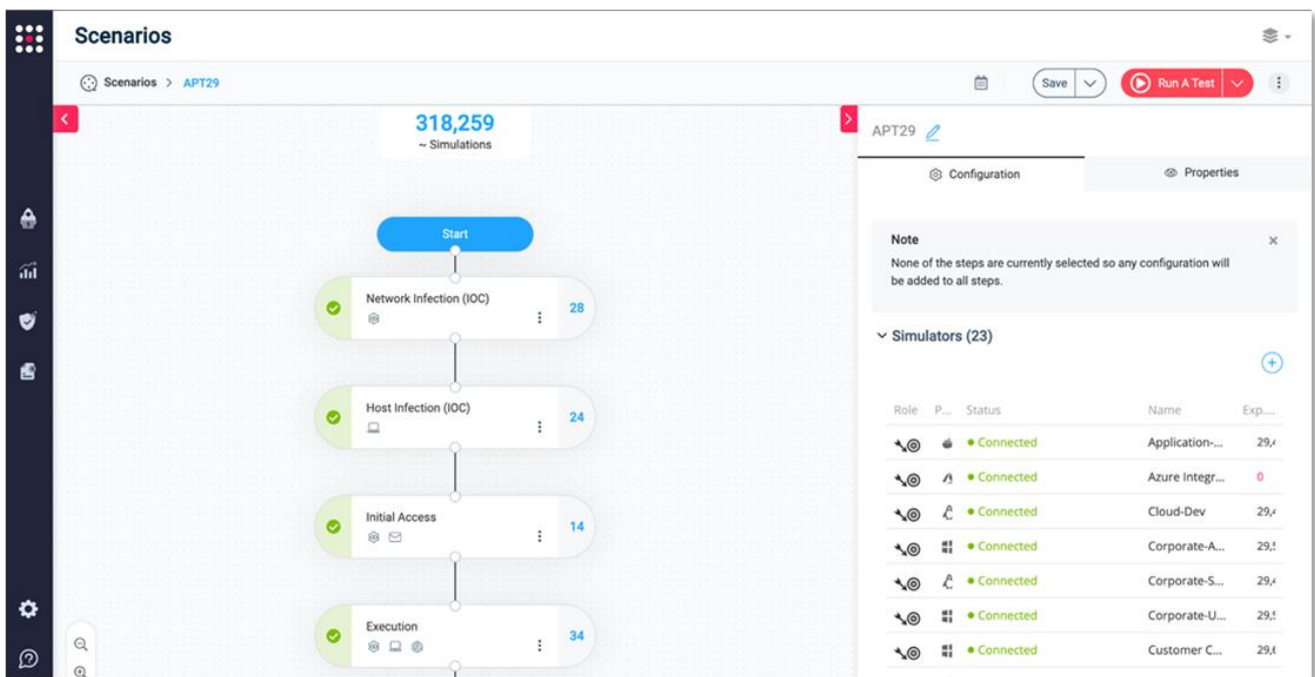
Figure 6. Hacker’s Playbook



Source: ESG, a division of TechTarget, Inc.

SafeBreach exposes the most powerful scenario- and attack-building tools through SafeBreach Studio (see Figure 7). SafeBreach Studio enables security experts to create custom scenarios and attacks from scratch using a no-code visual programming language that provides access to a vast library of attack steps and the ability to create custom attack steps of their own. Here, the most advanced users can create their own exploits and publish them to the attack playbook where they can be run against the environment like any other attack.

Figure 7. SafeBreach Studio



Source: ESG, a division of TechTarget, Inc.

## Why This Matters

Security tools must be useable for security specialists of all experience levels to provide the best value to an organization. Otherwise, security tool sprawl leads to increased overhead and complexity, adding complications to an already complicated profession.

SafeBreach offers strong capabilities at both ends of the spectrum. Less experienced employees use the pre-built scenarios to launch attacks from an easy-to-use interface. More advanced specialists use the Hacker's Playbook and SafeBreach Studio to build customized attacks from scratch. Together, both capabilities increase testing coverage and decrease risk without requiring multiple testing tools. They also help to prevent employee burnout by increasing efficiency.

### Contextual Intelligence to Reduce Risk

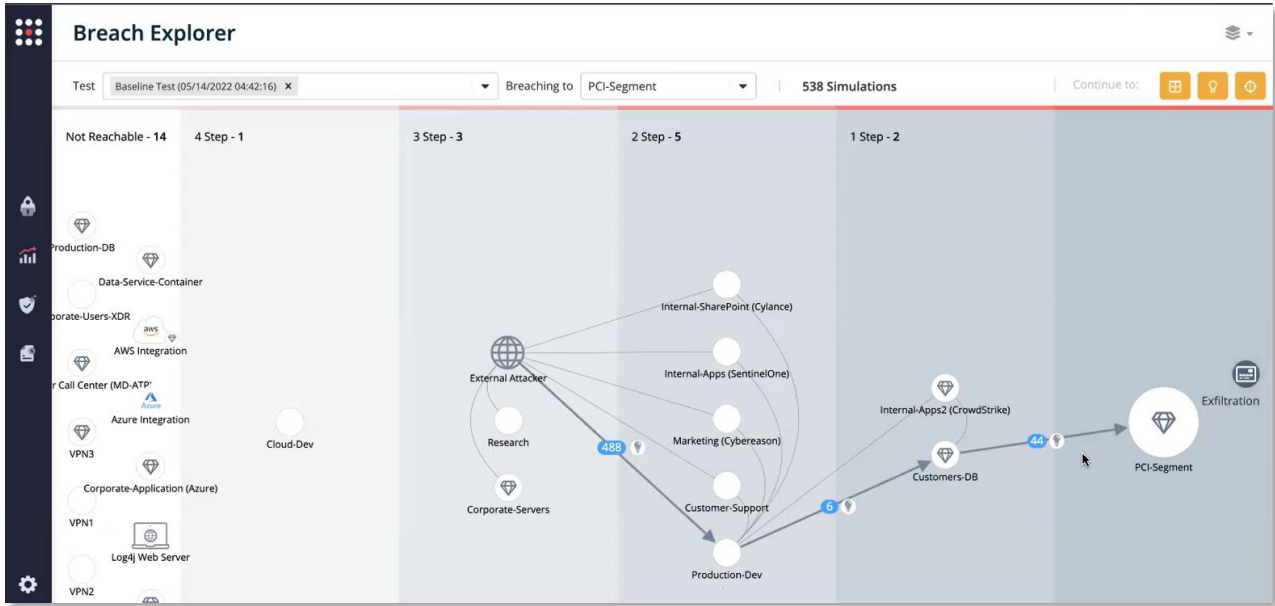
Finally, ESG examined the various reporting and dashboarding features in the SafeBreach platform. Without clear and intelligible reporting, it is difficult for an organization to understand its complete security posture. ESG validated SafeBreach to see how it helps organizations prioritize and mitigate risks through reporting and integration with downstream security tools.

#### Breach Explorer & MITRE ATT&CK Board – Understanding What Was Successful

Understanding which attack was successful and why it was successful is essential to securing complex environments. SafeBreach features many ways to identify gaps about where an organization's weaknesses lie, including visualizations provided by simulation results, Breach Explorer, and the MITRE ATT&CK board.

ESG observed Breach Explorer's ability to provide greater intelligence around real-world tactics used by attackers. Breach Explorer pivots through successful attacks from the attacker's point of view. It shows the steps necessary to complete the exploit and alternate paths the attacker could take to reach the same goal. Breach Explorer highlights the "leaks" within an environment so they can be closed (see Figure 8).

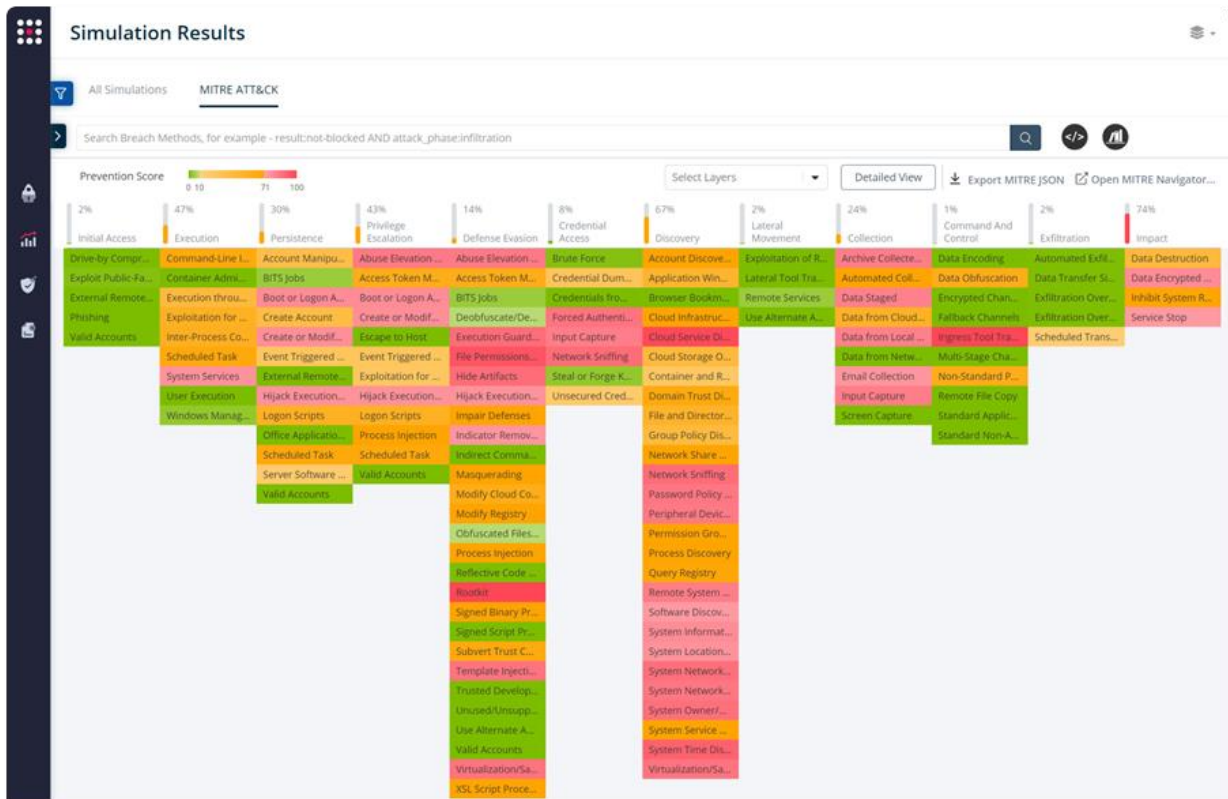
Figure 8. SafeBreach Breach Explorer



Source: ESG, a division of TechTarget, Inc.

A MITRE ATT&CK board maps MITRE attack tactics to various security controls, providing insight into which security controls successfully blocked and logged the attack and which attacks were missed entirely (see Figure 9).

Figure 9. MITRE ATT&CK Board

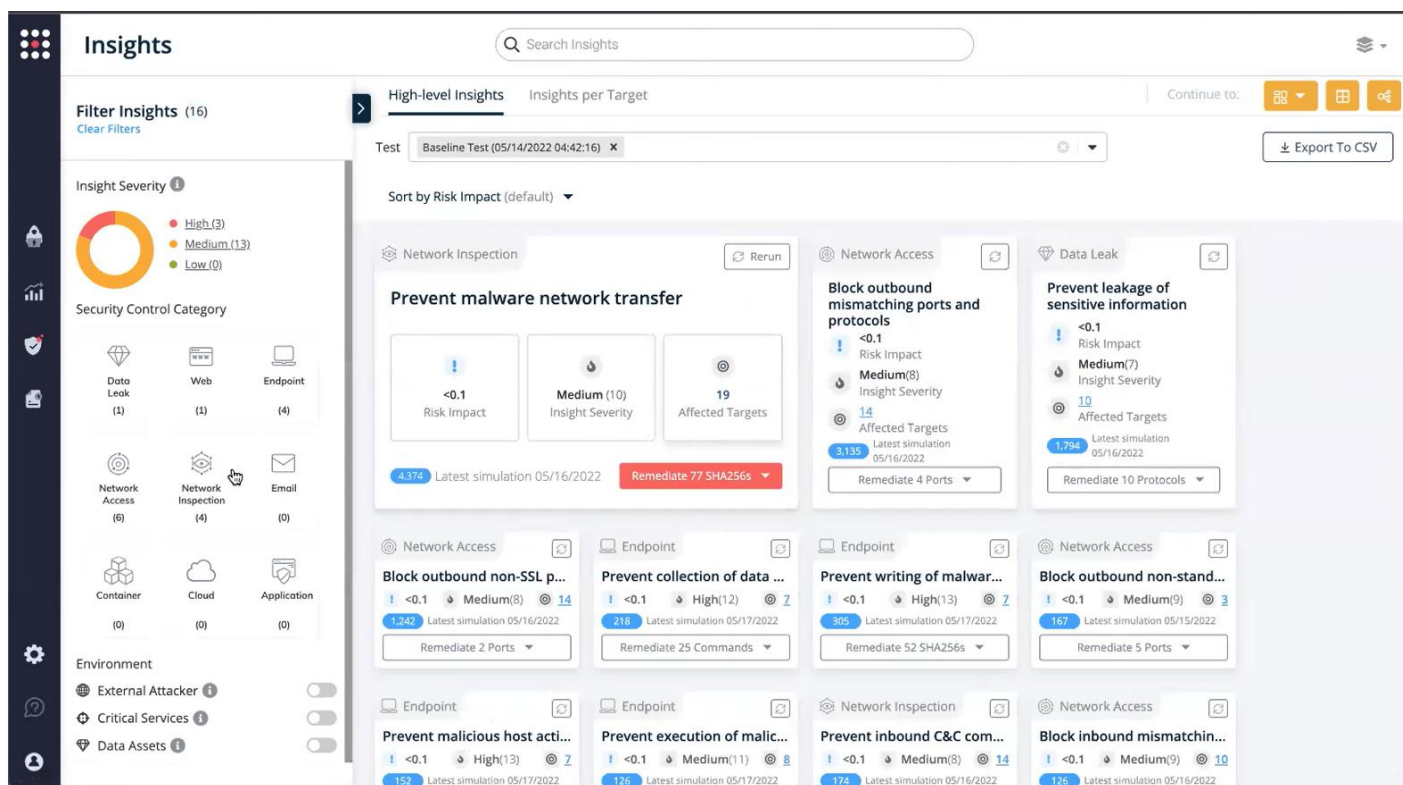


Source: ESG, a division of TechTarget, Inc.

## SafeBreach Insights

While a high-level security posture is invaluable to an organization, it doesn't always spell out next steps. The SafeBreach Insights module (see Figure 10) provides actionable intelligence that helps organizations prioritize risks and provides remediation steps. ESG observed over 100,000 attacks against a single environment reduced to 16 action items to remediate the critical risks.

**Figure 10. SafeBreach Insights Module**



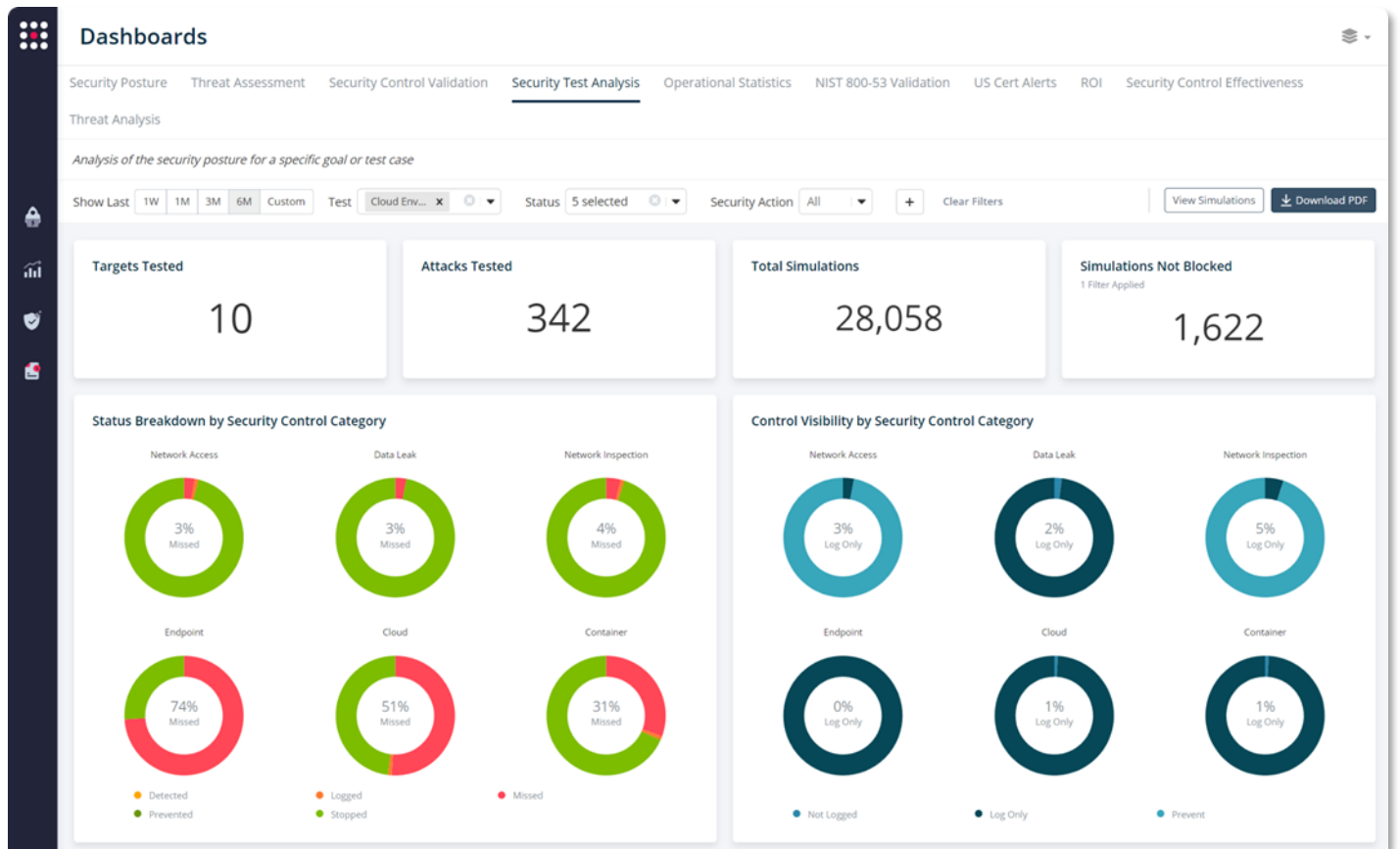
Source: ESG, a division of TechTarget, Inc.

SafeBreach integrates with downstream security tools such as SIEM and SOAR to close the vulnerability before an attack can exploit it. Antivirus tools such as Microsoft Defender can be updated by malware definitions provided by SafeBreach in the event a malware payload went undetected.

## Dashboards and Reporting

The dashboards provide high-level intelligence on the riskiest parts of the environment. Test results are broken down by business unit and security controls so that high-risk areas are seen immediately and then remediation can begin (see Figure 11). Dashboards with KPI reporting provide a quantitative view of an organization's security posture, which in turn can be sliced and diced based on criteria such as MITRE, security controls, business units, etc.

Figure 11. Test Results



Source: ESG, a division of TechTarget, Inc.

### Why This Matters

ESG research shows that 61% of organizations find it difficult to prioritize the actions that will reduce risk. Staying busy doing the wrong things won't lead to safer systems.

ESG validated that SafeBreach's dashboard and reporting system highlights the highest risks. SafeBreach provides a complete quantitative view of an organization's security posture with real-time results from running tests and data intelligence based on previous tests. Thousands of data points and simulations are boiled down to a manageable list of actions that will reduce risk immediately.

## The Bigger Truth

“How safe are we?” is a complex question that many organizations simply cannot answer with a high degree of certainty. Attackers become more sophisticated over time while information systems are becoming more complex and harder to defend. According to ESG research, 70% of organizations have more than 10 tools dedicated to tracking their overall security posture due to the complexity of modern environments.

SafeBreach simplifies the process of determining the extent to which an organization is vulnerable to attack, providing the ability to launch a variety of attack simulations based on real-world threats quickly and easily and alerting organizations to their vulnerabilities while providing the insight to mitigate them quickly and confidently. SafeBreach simulates APTs, ransomware, malware, and other modern attack methods. New attacks are added within 24 hours of US-CERT and FBI flash alerts.

SafeBreach reduces risk by highlighting the highest priority tasks that will immediately eliminate vulnerabilities. It becomes the only tool to evaluate and report on security control efficacy and provide a score of security posture while integrating with downstream security tools such as SIEM, SOAR, and workflow management applications. SafeBreach’s Breach Explorer gives security teams detailed intel about what path attackers could take through an organization’s environment to reach sensitive personal or business-critical data. Security teams can then use this information to close off those opportunities before a real attacker tries them.

The results that are presented in this document are based on testing in a controlled environment. Due to the many variables in each organization’s IT ecosystem, it is important to perform planning and testing in your own environment to validate the viability and efficacy of any solution.

ESG validated that SafeBreach can successfully answer the question of “How safe are we?” Its advanced attack tools and tests provide detailed intelligence to show an organization where its weaknesses lie and steps organizations can take to mitigate and eliminate them. If your organization is looking to gain a complete quantitative view of its security posture and gain practical insights into how to improve it, ESG believes you should seriously consider SafeBreach.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.’s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at [cr@esg-global.com](mailto:cr@esg-global.com).

The goal of ESG Validation reports is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Validation reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team’s expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.



Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

© 2022 TechTarget, Inc. All Rights Reserved.

